



Sheet 1 of 3

Form PTO-1449 (modified)

Attorney Docket No.  
ARC920010006US1Serial No.  
09/771,239LIST OF PATENTS AND PUBLICATIONS FOR  
APPLICANT(S) INFORMATION DISCLOSURE STATEMENT

(Use several sheets if necessary)

Applicant(s): LOTSPIECH et al.

Filing Date:  
01/26/2001Group Art Unit:  
2137

## U.S. PATENT DOCUMENTS

Examiner Initials	Document No.	Date	Name	Class	Subclass	Filing Date
20	US2002/0090090 A1	07/11/2002	Van Rijnsoever et al.	380	279	
20	6,397,329 B1	05/28/2002	Aiello et al.	713	155	
20	6,684,331 B1	01/27/2004	Srivastava	713	163	

## PUBLICATIONS / OTHER ART

Examiner Initials	Citation
20	PUBLICATION: "Secure Group Communications Using Key Graphs". Wong et al. Proceedings of ACM SIGCOMM. Pgs 1-12. September, 1998. Canada.
20	PUBLICATION: "Efficient Communication-Storage Tradeoffs for Multicast Encryption". Canetti et al. EUROCRYPT 1999. Pgs. 459-474.
20	PUBLICATION: "Key Establishment in Large Dynamic Groups Using One-Way Function Trees". McGrew et al. Submitted to IEEE Transactions on Software Engineering. Pgs. 1-13. May, 1999.
20	PUBLICATION: "Multicast Security: A Taxonomy and Some Efficient Constructions". Canetti et al. Proc. of INFOCOM. Vol. 2, pp. 708-716. New York, March 1999.
20	PUBLICATION: "Broadcast Encryption". CRYPTO 1992, LNCS Vol. 839, pp. 257-270, New York, March 1994.

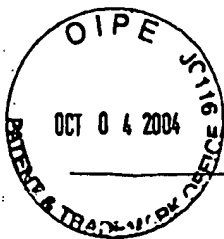
Examiner

  
Zachary  
Davis

Date Considered

11/15/04

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).



Sheet 2 of 3

Form PTO-1449 (modified)

Attorney Docket No.  
ARC920010006US1Serial No.  
09/771,239LIST OF PATENTS AND PUBLICATIONS FOR  
APPLICANT(S) INFORMATION DISCLOSURE STATEMENT

(Use several sheets if necessary)

Applicant(s):

LOTSPIECH et al.

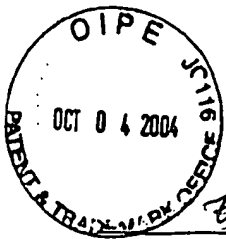
Filing Date:  
01/26/2001Group Art Unit:  
2137

## U.S. PATENT DOCUMENTS

Examiner Initials	Document No.	Date	Name	Class	Subclass	Filing Date
ZD	5812670	09/22/1998	Micali	380	25	
ZD	5675649	10/07/1997	Brennan et al.	380	21	
ZD	5748736	05-1998	Mittra	713	163	
ZD	6629243	09-2003	Kleinman	713	163	
ZD	6247127	06-2001	Vandergeest	713	100	
ZD	6285991	09-2001	Powar	705	76	
ZD	5241597	08/31/1993	Bright	380	21	

## PUBLICATIONS / OTHER ART

Examiner Initials	Citation
ZD	PUBLICATION: "Sequential Traitor Tracing". R. Safavi-Naini and Y. Wang. CRYPTO 2000, LNCS vol. 1880, PP. 316-332, 2000.
ZD	PUBLICATION: "Efficient Trace and Revoke Schemes". M. Naor and B. Pinkas. Financial Cryptography '2000, LNCS 1962, pp. 1-20, 2001.
ZD	PUBLICATION: "Efficient Methods for Integrating Traceability and Broadcast Encryption". E. Gafni, Jessica Staddon and Yiqun Lisa Yin. CRYPTO '99, Springer-Verlag LNCS 1666, pp. 372-387, 1999.
ZD	PUBLICATION: "Trials of Traced Traitors". Birgit Pfitzmann. Workshop on Information Hiding, Cambridge, UK, LNCS, Vol. 1174, Springer-Verlag, pp. 1-16, 1996.
ZD	PUBLICATION: "Digital Signets: Self-Enforcing Protection of Digital Information". C. Dwork, J. Lotspiech and M. Naor. 28 <sup>th</sup> Symposium on the Theory of Computation, pp. 489-498, 1996.
ZD	PUBLICATION: "An Efficient Public Key Traitor Tracing Scheme". D. Boneh and M. Franklin, Proceedings CRYPTO '99, LNCS, Vol. 1666, Springer-Verlag, pp. 1-13, i-iv, 1999.



	PUBLICATION: "Collusion-Secure Fingerprinting for Digital Data". D. Boneh and J. Shaw. IEEE Transactions on Information Theory, Vol. 44, No. 5, pp. 1897-1905, 1998.
20	PATENT APPLICATION: "Forensic Media Key Block for Identifying Compromised Keys". Lotspiech. Co-pending application serial no. 09/564,658, filed May 3, 2000.
20	PUBLICATION: "Threshold Traitor Tracing". M. Naor and B. Pinkas, CRYPTO '98, LNCS vol. 1462, pp. 502-517, 1998.
20	PUBLICATION: "Efficient Dynamic Traitor Tracing". O. Berkman, M. Parnas and J. Sgall. Proceedings of the 11 <sup>th</sup> ACM-SIAM Symp. On Discrete Algorithms (SODA), PP. 586-595, 2000.
20	PUBLICATION: "Tracing Traitors". B. Chor, A. Fiat, M. Naor and B. Pinkas. IEEE Transactions on Information Theory, Vol. 46, No. 3, May 2000.
20	REPORT: "Key Management for Multicast: Issues and Architectures". D. Waller, E. Harder, and R. Agee. National Security Agency, pp. 1-19, June 1999.
20	PUBLICATION: "On the Generation of Cryptographically Strong Pseudorandom Sequences". Adi Shamir, ACM Transactions on Computer Systems, vol. 1, no. 1, pp. 38-44, February 1983.
20	PUBLICATION: "Tracing Traitors". B. Chor, A. Fiat and M. Naor. CRYPTO '94, Incs Vol. 839, pp. 257-270, 1994.

Examiner

*[Signature]*  
Zachary Davis

Date Considered

11/15/04

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).